REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
13/Aug/2001	THESIS	

4. TITLE AND SUBTITLE
CYBERESPIONAGE UNDER INTERNATIONAL LAW APPLICABLE IN CYBERSPACE

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
MAJ ROMERO JORGE H

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
GEORGETOWN UNIVERSITY

8. PERFORMING ORGANIZATION REPORT NUMBER
CI01-200

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
THE DEPARTMENT OF THE AIR FORCE
AFIT/CIA, BLDG 125
2950 P STREET
WPAFB OH 45433

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Unlimited distribution
In Accordance With AFI 35-205/AFIT Sup 1

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE		64	19b. TELEPHONE NUMBER *(Include area code)*

GEORGETOWN UNIVERSITY
LAW CENTER

CYBERESPIONAGE 2010:
Is the Current Status of Espionage Under International Law Applicable in Cyberspace?

Jorge H. Romero
LLM in International and Comparative Law
Graduate Paper

International Law
at the Turn of the Century Seminar
Professor Dalton

Final Version
30 April 2001

CYBERESPIONAGE 2010:
Is the Current Status of Espionage Under International Law Applicable in Cyberspace?

Jorge H. Romero
LLM in International and Comparative Law
Graduate Paper

International Law
at the Turn of the Century Seminar
Professor Dalton

The views expressed in this paper are those of the author and do not necessarily reflect the official policy or position of the Department of the Air Force, the Department of Defense or the United States Government.

ABSTRACT

In this thesis I will argue that the current status of espionage under international law is applicable in cyberspace. Therefore, there is no need to reinterpret espionage under international law in cyberspace. There is no need for new treaties to regulate or control espionage in cyberspace among nations. At the present time, espionage is legal under international law, or stated in another way, there are no international law prohibitions against espionage. Presently, there is a discussion about the applicability of various areas of the law in cyberspace. One school of thought says that new laws are needed to adapt an area of law into cyberspace. The other school of thought believes that there is no need for new laws – that current principles of laws can be analogized into cyberspace. The first school of thought is led by Professor Lawrence Lessig. The second school of thought is led by Judge Frank Easterbrook. I will argue that Judge Easterbrook's position should be followed in the area of espionage in cyberspace (hereinafter I will refer to this concept as *"cyberespionage"*). Finally, I will examine the consequences of cyberespionage to the present framework of espionage and international law.

Index

Computer espionage and computer network attack are two of the most urgent issues facing warfighters, decision-makers, and international lawyers today.
- Walter Gary Sharp, Sr.
Cyberspace and the Use of Force[1]

I. Introduction

Espionage is an integral tool of nations.[2] Intelligence collection and espionage have always been part of human history.[3] After all, in one of the earliest Bible stories Joshua sent two Israelites to spy on Jericho.[4] Throughout history, espionage has been conducted during peacetime and wartime.[5] The methods to carry out espionage have also changed throughout history.[6] Nations have taken advantage of technological advances to improve their intelligence collection and espionage.[7] First, it was simple physical surveillance espionage.[8] Then, with the advent of electronic devices, electronic espionage was born.[9] Following the invention of airplanes and submarines, nations resorted to aerial and submarine espionage.[10] Once space flights were possible, space

---

[1] WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE 123 (1999).

[2] *See generally,* MICHAEL HERMAN, INTELLIGENCE POWER IN PEACE AND WAR (1996).

[3] *See generally,* FRANCIS DVORNIK, ORIGINS OF INTELLIGENCE SERVICES (1974).

[4] *Joshua* Chapter 2 (Revised Standard Version, Catholic Edition).

[5] HERMAN, *supra* note 2, at 9.

[6] *See generally,* DVORNIK, *supra* note 3; JOHN M. CARROLL, SECRETS OF ELECTRONIC ESPIONAGE (1966); ALLEN DULLES, THE CRAFT OF INTELLIGENCE (1963).

[7] *See generally,* SHERRY SONTAG & CHRISTOPHER DREW, BLIND MAN'S BLUFF: THE UNTOLD STORY OF AMERICAN SUBMARINE ESPIONAGE (1998); WILLIAM E. BORROWS, DEEP BLACK: SPACE ESPIONAGE AND NATIONAL SECURITY (1986); FRANCIS GARY POWERS, OPERATION OVERFLIGHT (1970); CARROLL, *supra* note 6; WILLIAM BONI & DR. GERALD KOVACICH, NETSPIONAGE: THE GLOBAL THREAT TO INFORMATION (2000); JEAN GUISNEL, CYBERWARS: ESPIONAGE ON THE INTERNET (2000).

[8] *See generally,* DVORNIK, *supra* note 3; DULLES, *supra* note 6.

[9] *See generally,* CARROLL, *supra* note 6.

espionage was surely to follow.[11] For all the above types and methods of espionage and collection of intelligence, "there is a customary practice of nations, and is regarded as a vital necessity in the national security process."[12] Enter the Internet and cyberspace.

Presently, there is a debate about the applicability of various areas of the law into cyberspace. From intellectual property law to choice-of-law, scholars and professors are debating how the traditional fields of law apply (or do not apply) to the Internet and cyberspace.[13] This debate can roughly be categorized into two schools of thought. One school of thought says that new laws are needed specific to cyberspace. The other school of thought believes that there is no need for new laws – that current principles of laws can be analogized into cyberspace. The first school of thought is led by Professor Lawrence Lessig.[14] Judge Frank H. Easterbrook leads the second school of thought.[15] I will argue that the second school of thought – that current principles of laws can be analogized into cyberspace – should be the analytical framework for discussing and thinking about

---

[10] *See generally,* THE TRIAL OF THE U-2, EXCLUSIVE AUTHORIZED ACCOUNT (1960); SONTANG & DREW, *supra* note 7; DICK VAN DER ART, AERIAL ESPIONAGE: SECRET INTELLIGENCE FLIGHTS BY EAST AND WEST (1986).

[11] *See generally,* BURROWS, supra note 7.

[12] W. Hays Parks, *The International Law of Intelligence Collection*, in NATIONAL SECURITY LAW 433 (John Norton Moore et al. eds., 1990).

[13] DAVID R. KOEPSELL, THE ONTOLOGY OF CYBERSPACE: PHILOSOPHY, LAW, AND THE FUTURE OF INTELLECTUAL PROPERTY 1 (2000). *See also*, MARK A. LEMLEY ET AL., SOFTWARE AND INTERNET LAW (2000); KATHARINA BOELER-WOELKI & CATHERINE KESSEDJIAN (EDS.), INTERNET: WHICH COURT DECIDES? WHICH LAW APPLIES? (1998); ULRICH SIEBER, THE INTERNATIONAL EMERGENCE OF CRIMINAL INFORMATION LAW (1992).

[14] Professor Lessig is Professor of Law at Harvard. His seminal article on this issue is *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 50 (1999). *See also,* LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999); *The Path of Cyberlaw*, 104 YALE L.J. 1743 (1995); *The Zones of Cyberspace*, 48 STAN. L. REV. 1403 (1996).

[15] Judge Easterbrook is judge of the United States Court of Appeals for the Seventh Circuit. His seminal article on this issue is *Cyberspace and the Law of the Horse*, U. CHI. LEGAL F. (1996).

espionage in cyberspace. Hereinafter I will refer to this concept of espionage in cyberspace as *"cyberespionage"*.

I present my analysis in eight sections. In section II, I will show the urgency to understand cyberespionage and current issues regarding cyberespionage. At the present time it appears that increasingly more nations are developing cyber forces and the international community is willing to enter into treaties regulating conduct in cyberspace.

In section III, I will define and explain the current status of espionage under international law. I will present the status of espionage under peacetime and armed conflict.

In section IV, I will briefly explain certain concepts and ideas about cyberspace that will illuminate the thesis and proposition of this paper. This section will serve as an introduction to key principles about cyberspace directly applicable to espionage and cyberespionage. The main concepts to understand are: Information Operations; Information Warfare; Cyberwar; Netwar; Cyberterrorism; Computer Network Espionage; and Computer Network Attack. Other cyberspace concepts applicable to espionage will be defined throughout the paper.

In section V, I will introduce both sides of the argument developed by Professor Lessig and Judge Easterbrook. I will explain why some scholars believe we need new laws specific to cyberspace. I also will explain why other scholars believe that the law can be adapted or analogized into cyberspace. I will explain both sides mainly using Professor Lessig and Judge Easterbrook's writings about this debate. This section will develop a framework of analysis to explain (in section VI) why new international law or treaties are not needed in the area of cyberespionage.

In section VI, I will argue that the present status of espionage under international law is applicable in cyberspace. Basically, I will use the framework of analysis developed in section V and demonstrate that there is no need for new international law or treaties in order to understand (and accept) espionage in cyberspace.

In section VII, I will explain that even if the current status of espionage is applicable in cyberspace, the consequences can be more dangerous than normal or established methods of espionage. Specifically, I will explain the dangers of a computer network espionage being misunderstood or interpreted by the targeted nation as a computer network attack.

In section VIII, I will explain the possible criminal liability for cyberspies under foreign domestic laws against espionage. This section will place espionage in the proper international context: although there are no prohibitions against espionage under international law, cyberspies must be aware that they may be criminally liable under foreign domestic laws and should protect themselves accordingly.

Finally, in section IX, I will explore the future of cyberespionage and international law. Quantum computers and quantum cryptography will really have a profound impact on international relations and international law – whoever creates a quantum computer will basically control cyberspace – and this is not science fiction.

Appendix 1 contains a summary of the thesis in a chart form. It shows at a glance a comparison of the main elements and characteristics of espionage during peacetime, wartime, and in cyberspace. It also includes a summary of the main treaties and documents related to espionage in peacetime and wartime.

The current status of espionage under international law should be applicable in cyberspace. Therefore, there is no need to create new international law or treaties to control or regulate espionage in cyberspace.

II. Urgency to Understand Cyberespionage

There is an urgent need to understand cyberespionage and its relationship to international law. Just in January 2001, a news report titled "DOD Exec to Thwart Cyberspies," stated in part:

> The Pentagon wants to create a national counterintelligence executive to help Defense Department tap the abilities of all national counterintelligence forces and fend off ***cyberspies***. The Pentagon disclosed its intent to create the new position in its 2001 'Annual Report to the President and Congress,' a yearly outline of the department's goals and accomplishments. The department has worked with the FBI and the CIA to develop a new counterintelligence strategy known as CI 21, which is designed to fend off ***spies who exploit modern computer technology and the Internet to steal U.S. secrets***.[16]

A. Misconceptions About Espionage[17]

When confronted with the issue and consequences of espionage, most people tend to think of it as completely illegal or unethical conduct by states. But, espionage has an important role in the national security of nations. Espionage can provide security by

---

[16] George I. Seffers, *DOD Exec to Thwart Cyberspies,* FEDERAL COMPUTER WEEK, January 18, 2001, at http://www.fcw.com/fw/articles/2001/0115/web-dod-01-18-01.asp (emphasis mine).

[17] An excellent source of background information regarding espionage can be found in the bibliographical work by James D. Calder. His bibliographical work on espionage contains 10,369 annotated bibliographical entries of journals and magazine scholarship articles on espionage. JAMES D. CALDER, INTELLIGENCE, ESPIONAGE AND RELATED TOPICS: AN ANNOTATED BIBLIOGRAPHY OF SERIAL JOURNAL AND MAGAZINE SCHOLARSHIP 1844-1998 (1999).

alerting the state of hostile intentions by another country.[18] "Peace-time espionage has been justified on the basis that it has always been the common practice of all states, and because of the necessity for self-defense and the need to maintain the balance of power."[19]

Sound foreign policy requires proper intelligence.[20] Wars and surprise armed attacks could be prevented with proper intelligence – just remember Pearl Harbor.[21] "The Pearl Harbor disaster produced a lasting U.S. preoccupation with warning against surprise attack."[22] Espionage and intelligence collection will mean something different to each nation. Perceptions by states are important factors, also. "Intelligence's importance in this narrow context depends upon threats and vulnerabilities and national perceptions of them. Those states with the biggest threats, internal or external, have the biggest reasons for taking intelligence seriously."[23] Even after the Cold War, the United States still needs excellent intelligence collection and espionage. "Thus the United States as a still active superpower seeks world class intelligence with worldwide coverage, despite the absence after the Cold War of any significant international threats and vulnerabilities (though terrorism against US forces and civilians overseas provides specific reasons for extensive US intelligence against terrorist targets)."[24]

---

[18] HERMAN, *supra* note 2, at 342.

[19] Elmar Rauch, *Espionage*, ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW, MAX PLANCK INSTITUTE FOR COMPARATIVE PUBLIC LAW AND INTERNATIONAL LAW, VOLUME 2, AT 116.

[20] Herbert Scoville, Jr., *Is Espionage Necessary for Our Security?* 54 FOREIGN AFFAIRS 482 (1976).

[21] HERMAN, *supra* note 2, at 342.

[22] *Id.*

[23] *Id.*, at 343.

[24] *Id.*, at 344.

A senior intelligence official described intelligence's national value in the post-Cold War world:

> The general effect of intelligence knowledge is also to incline national governments to behave better, in international security terms, than they would without it. Most intelligence collection that contributes to this knowledge operates over long distances and is unspecific in its targets. Intelligence as a whole tends to improve international society and does not introduce new tensions within it; it is an unprovocative form of national power.[25]

B. Threats to National Security

One of the most important developments affecting international law and international relations at the end of the twentieth century is the Internet and cyberspace. Cyberspace and the Internet are redefining and affecting many areas, like intellectual property.[26] But cyberspace is also affecting our national security. Every day we hear or read news about computer hacking and the threat to our computers, privacy, industry, and our lives in general. We also hear about the increasing threat of computer-related crimes[27] to our national security or critical infrastructure.[28] The news media is saturated with these stories. In many instances, the media reports on amazing cases of computer espionage, computer hacking, and computer security breaches that make us wonder what

---

[25] *Id.*, at 385.

[26] *See generally,* LEMLEY ET AL, *supra* note 13; Lessig, *The Law of the Horse: What Cyberlaw Might Teach, supra* note 14; and DOROTHY DENNING, INFORMATION WARFARE AND SECURITY (1998).

[27] *See generally,* DAVID H. FREEMAN & CHARLES C. MANN, AT LARGE (1997); CLIFF STOLL, THE CUCKOO'S EGG (1989); DAVID ICOVE ET AL, COMPUTER CRIME (1995); DONN PARKER, FIGHTING COMPUTER CRIME (1998); RICHARD POWER, TANGLED WEB (2000); WINN SCHWARTAU, INFORMATION WARFARE (1996); WINN SCHWARTAU, CYBERSHOCK (2000).

[28] Presidential Policy Directive 63, May 1998 [*hereinafter* PDD 63] "calls for a national effort to assure the security of the increasingly vulnerable and interconnected infrastructures of the United States. Such infrastructures include telecommunications, banking and finance, energy, transportation, and essential government services" *reprinted in* YONAH ALEXANDER & MICHAEL SWETNAM, CYBER TERRORISM AND INFORMATION WARFARE: VOL I, ASSESSMENT OF CHALLENGES 163 (1999).

will be next. Not everything being reported is media hype. Increasingly, we see government officials uttering statements that would provoke chills on anyone's spine. For example, on August 25, 2000, Secretary of Defense William Cohen stated: "We're looking at what I call a 'superpower paradox....There is no other country that can challenge us directly. So they look for indirect ways to challenge us....That can come in the form of chemical or biological or even cyber [warfare]."[29] Also, words from then-President Clinton should be enough to make us aware of the threat in cyberspace. President Clinton requested from Congress US$2.8 billion to defend the United States against various terrorist threats, including protection of our computer networks. The Internet news site reporting this event stated: "[President] Clinton described a world of frightening terror scenarios involving nerve gas, germ attacks, and computer hacking that, until now, have largely been the province of thriller novels."[30] Statements from government officials are not the only source warning us of this threat. Government documents, studies, and reports (not to mention non-government sources[31]) continue to appear, reinforcing the fact that computer-related crimes pose a threat to our critical infrastructure.

---

[29] *US Official: Superpower Status Risks Cyberattack,* CNN NEWS, August 25, 2000, http://www.cnn.com/2000/TECH/computing/08/25/cyberattack.superpower.idg/index.html

[30] *Clinton Combats Cyberterrorism*, WIREDNEWS, January 22, 1999, http:/www.wirednews.com/news/politics/0,1283,17494,00.html.

[31] *See generally,* DENNING, *supra* note 26; YONAH ALEXANDER & MICHAEL SWETNAM, CYBER TERRORISM AND INFORMATION WARFARE, VOL. III, CRITICAL INFRASTRUCTURE PROTECTION ISSUES (1999); CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES TASK FORCE REPORT, CYBERCRIME...CYBERTERRORISM....CYBERWARFARE....AVERTING AN ELECTRONIC WATERLOO (1998) [*hereinafter* Task Force Report]; SCHWARTAU, INFORMATION WARFARE, *supra* note 27; SCHWARTAU, CYBERSHOCK, *supra* note 27.

The information referenced above provides us with an idea of how the U.S. government views and perceives the threat of computer-related crimes and activities against the critical infrastructure. There are many in the non-government sector that have sounded alarms and warnings. It appears that non-government studies agree with the fact that, unless proper precautions and actions are taken, the U.S. risks facing an "electronic Waterloo"[32] or "electronic Pearl Harbor".[33] Whether or not the threat has been exaggerated, the fact is that based on all available studies, reports, and statements from government officials (including the President and Vice-President of the United States) we can but ponder when such an attack or attacks will take place. Cyberspace and the Internet pose a serious threat to our national security, but it also offers an opportunity for the United States to obtain information from other countries through cyberespionage.

Cyberspace issues are permeating all aspects of the United States national security.[34] Just recently, it was reported that the United States military "has a new mission: be ready to launch a cyberattack against potential adversaries, some of whom are stockpiling cyberweapons."[35] The news article explains that "such an attack would likely involve launching massive distributed denial-of-service assaults, unleashing

---

[32] *See generally, Id.*, TASK FORCE REPORT.

[33] *See generally,* CYBERWAR: SECURITY, STRATEGY AND CONFLICT IN THE INFORMATION AGE (Alan D. Campen et al. eds., 1996).

[34] For an overview of issues regarding information warfare and the law, see in general, Richard W. Aldrich, *Legal Implications of Information Warfare*, INSS Occasional Paper 9, USAF INSTITUTE FOR NATIONAL SECURITY STUDIES (1996); Anthony D'Amato, *International Law, Cybernetics, and Cyberspace,* NAVAL WAR COLLEGE INTERNATIONAL LAW STUDIES, VOLUME 7 (2000); Michael J. Robbat, *Resolving the Legal Issues Concerning the Use of Information Warfare In the International Forum*, 6 B.U. J. SCI & TECH. L. 10, at paragraph 48 (2000).

[35] Ellen Messmer, *U.S. Army Kicks-starts Cyberwar Machine,* Network World Fusion News, November 20, 2000, at http://www.nwfusion.com/news/2000/1120cyberattack.html?nf.

crippling computer viruses or Trojans, and jamming the enemy's computer systems...."[36] Further, the Secretary of Defense, Donald Rumsfeld, stated that part of the new challenges will be information warfare.[37] Therefore, there should be an urgency in understanding national security, including espionage, in cyberspace.

The United States government estimates that about 120 countries have or are developing information warfare systems, including China and France.[38] Also, "a step towards deterrence was taken in 1998 when CIA Director George Tenet announced that the United States was devising a computer program that could attack the infrastructure of other countries."[39]

The above analysis and information means one thing: nations and armed forces around the globe, including China, are increasingly moving towards developing cyber forces.[40] Therefore, the question of whether the current status of espionage under international law is applicable into cyberspace and/or whether new rules in this area are needed, is particularly pressing.

---

[36] *Id.*

[37] ABC NIGHTLY NEWS, December 28, 2000 (broadcasted in a local Washington D.C. television affiliate).

[38] John Christensen, *Bracing for Guerrilla Warfare in Cyberspace*, CNN NEWS, April 6,1999, at http://www.cnn.com/TECH/specials/hackers/cyberterror/.

[39] *Id.*

[40] Jason Sherman, *Report: China Developing Force To Tackle Information Warfare*, DEFENSE NEWS, 27 November 2000, at 1. This report states that "China is developing a strategic information warfare unit to neutralize the military capabilities of technologically advanced foes, according to a new report. The unit, dubbed Net Force, will wage combat through computer networks to manipulate enemy information systems spanning spare parts delivery to fire control and guidance systems...."

C. International Community Efforts to Control Cyberspace

Not surprisingly, "As soon as the concept of 'information warfare' began to receive broad press coverage, discussion began of negotiating a treaty that would prohibit or restrict it. A draft treaty text that circulated on the Internet in 1995 said simply, 'The Parties to this Convention agree not to engage in information warfare against each other'."[41]

Another effort was led by the Russians in 1998:

> The effort by Russia in the fall of 1998 to get the United Nations to take a firm stand on restricting information warfare produced only a resolution passed by the General Assembly on 4 January 1999 entitled 'Developments in the field of information and telecommunications in the context of international security,' which 'calls upon Member States to promote at multilateral levels the consideration of existing and potential threats in the field of information security....'[42]

A third proposal calls for an Information Operations Treaty to control or regulate information operations and warfare.[43] The proponents state that "It is too late to put the Information Operations (IO) genie back in the bottle....The purpose....is to make a case for the establishment of treaty guidelines for the use of Information Operations...."[44] Other efforts include a treaty to combat cyber crimes proposed by the Europeans.[45]

---

[41] DOD OFFICE OF GENERAL COUNSEL, AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 45 (1999).

[42] *Id.*, at 53 (citing from United Nations resolution U.N. Doc. A/RES/53/70, 1999).

[43] *Developing an Information Operations Treaty*, at http://www.infowar.com/info_ops/info_ops_030399a_j.shtml

[44] *Id.*

[45] *See generally* the Council of Europe, *Draft Convention on Cyber-crime* (Draft No 25 REV. 5), at http://conventions.coe.int/treaty/EN/cadreprojets.htm.

As we shall see in more detail below, cyberespionage is a form of information warfare.[46] Therefore, any attempt to regulate information warfare at the international level could affect how nations carry out cyberespionage. Such attempt to control or regulate espionage in cyberspace is misguided. As I argue in this paper, the current status of espionage under international law should be applicable in cyberspace and no new treaties or regulation to control espionage in cyberspace is necessary.

III. Espionage Under Present International Law

Espionage has been defined as "a method of information gathering."[47] According to the Max Planck Institute for Comparative Public Law and International Law, there are three categories of intelligence collection: (1) aerial and space reconnaissance; (2) electronic eavesdropping; and (3) the secret agent.[48] The Max Planck Institute divides or distinguishes between espionage in time of war and peacetime espionage.[49] The Department of Defense Office of General Counsel also distinguishes between espionage during armed conflict and espionage in peacetime.[50] "It is a continuous process, in peace and war, although emphasis with regard to information sought will vary depending on need and assets available."[51]

---

[46] DENNING, *supra* note 26, at 31-34. *See also* Martin C. Libicki, *What is Information Warfare?* NATIONAL DEFENSE UNIVERSITY Chapters 4 and 8 (1995), *available at* http://www.ndu.edu/inss/actpubs/act003/a003ch01.html.

[47] ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW, *supra* note 19, at 114.

[48] *Id.*

[49] *Id.*, at 114-116.

[50] DOD OFFICE OF GENERAL COUNSEL, *supra* note 41, at 43.

[51] Parks, *supra* note 12, at 433.

Espionage does not violate international law.[52] According to Lauterpacht's edition of Oppenheim:

> Spies are secret agents of a state sent abroad for the purpose of obtaining clandestinely information in regard to military or political secrets. Although all states constantly or occasionally send spies abroad, and although it is not considered wrong morally, politically, or legally to do so, such agents have, of course, no recognized position whatever according to international law, since they are not agents of states for their international relations.[53]

A. Espionage Under Peacetime

Peacetime espionage must be distinguished from wartime espionage.[54] "Some authors consider that what applies (in espionage) in wartime does not apply in peace-time."[55] Nations have conducted espionage during peacetime all throughout history[56] "and regarded [it] as a vital necessity in the national security process."[57] Further, "Peace-time espionage has been justified on the basis that it has always been the common practice of all states, and because of the necessity for self-defense and the need to maintain the balance of power."[58] The basic general rule is that espionage is not prohibited by international law. According to the Max Planck Institute, "there are

---

[52] Commander Roger D. Scott, *Territorial Intrusive Collection and International Law*, 46 A.F. L. REV 217, 222 (1999).

[53] 1 L. OPPENHEIM'S INTERNATIONAL LAW §455, at 862 (H. Lauterpacht ed., 8th ed. 1955).

[54] ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW, *supra* note 19, at 116.

[55] *Id.*, at 114. *See also*, JOHN KISH, INTERNATIONAL LAW AND ESPIONAGE 123 (1995).

[56] Commander Scott, *supra* note 52, at 218.

[57] Parks, *supra* note 12, at 433.

[58] ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW, *supra* note 19, at 116.

insufficient grounds to warrant the statement that international law does not permit espionage in peace-time."[59]

The above analysis does not end the discussion about espionage during peacetime. Although international law does not prohibit espionage, there are other factors that come into play depending on where and how espionage is conducted. To that end, espionage during peacetime must be understood and analyzed according to location and method: (1) national territory; (2) national airspace; (3) high seas; and in (4) space. This analysis of espionage according to location and method will facilitate our study of espionage in cyberspace, because cyberspace could be viewed as a fifth "location and/or method" where espionage is carried out.

1. Espionage in National Territory

International law recognizes the general principle of exclusive sovereignty over national territory.[60] This means that each state has control over its territory to the exclusion of all other states.[61] This principle of territorial sovereignty was recognized in 1919 in the Covenant of the League of Nations.[62] The principle of territorial integrity was again affirmed in Article 2(4) of the Charter of the United Nations. Article 2(4) states: "All members shall refrain in their international relations from the threat or use of

---

[59] *Id.*

[60] KISH, *supra* note 55, at 83.

[61] *Id.*

[62] Professor Kish cites the Covenant of the League of Nations, Article 10. Article 10 provides for the protection of territorial sovereignty in the following manner: "The members of the League undertake to respect and preserve as against external aggression the territorial integrity and existing political independence of all Members of the league." Versailles, 28 June 1919 (Treaty Series, 1919/4) at 25.

force against the territorial integrity or political independence of any state...."[63] According to Professor John Kish, "The material scope of Article 2(4) has further important implications. The concept of territorial integrity negates the general permissibility of strategic observation in foreign territory and indicates the requirement of special consent by the territorial state."[64]

In contrast to the above, Thomas Wingfield states that the "1961 Vienna Convention on Diplomatic Relations explicitly recognizes the well-established right of nations to engage in espionage during peacetime, and the practice of states has specifically recognized a right to engage in such clandestine intelligence collection activities as an inherent part of foreign relations and policy."[65] Specifically, Article 3(1)(d) of the Vienna Convention on Diplomatic Relations provides:

> (1) The functions of a diplomatic mission consist, inter alia, in:....(d) Ascertaining by all lawful means conditions and developments in the receiving state, and reporting thereon to the Government of the sending state...."[66]

According to Professor Kish, Article 3(1)(d) allows for the collection of intelligence by diplomatic personnel. Professor Kish explains:

> The positive function of ascertaining conditions and developments in the receiving State is intentionally formulated in such general terms as to cover the entire notion of diplomatic observation without any substantive limitation. In the absence of such limitations, the Convention thus implies the permissibility of the diplomatic observation of not only such neutral areas....but also such politically sensitive areas as public order, foreign

---

[63] U.N. CHARTER art. 2(4).

[64] KISH, *supra* note 55, at 84.

[65] THOMAS C. WINGFIELD, THE LAW OF INFORMATION CONFLICT 350 (2000).

[66] KISH, *supra* note 55, at 55.

policy and defence.[67]

Professor Kish explains the benefits allowed by such language in the Vienna Convention on Diplomatic Relations:

> Although the exercise of this diplomatic function by the sending state naturally affects the national security of the receiving state, the dual status of every state as both sending and receiving state ensures the reciprocal and, therefore, the equitable application of the rule of diplomatic observation. Every state is meant to be compensated for the intrusion into its national security in its capacity as receiving state by benefiting from diplomatic observation in its capacity as sending state.[68]

The above interpretation fits with the international law doctrine called *"tu quoque,"* or "a nation has no standing to complain about a practice in which it itself engages."[69] This international law doctrine and the explanation by Professor Kish does not mean that an intrusion by one state into the territory of another state to conduct espionage is a lawful intervention. What all the above means is that there is no present international law prohibiting espionage, despite the acknowledgment by nations that espionage could constitute an unlawful intervention some times. Or, as recently explained, "The traditional doctrinal view is that intelligence gathering within the territory of other states during peacetime constitutes an unlawful intervention. The essence of the international law norm against peacetime espionage is the lack of respect for the territorial boundaries of another sovereign....Notwithstanding the apparent clarity

---

[67] *Id.*

[68] *Id.*

[69] DOD OFFICE OF GENERAL COUNSEL, *supra* note 41, at 43.

of the traditional view, espionage is not prohibited by any international convention because all states have an interest in conducting such activity."[70]

2. Espionage in National Airspace

It is held under customary international law that territorial sovereignty also extends to national airspace above national territory.[71] "The general practice of states manifests the consistent recognition of territorial sovereignty over national airspace in customary international law."[72] National security is the major consideration for preserving sovereignty over national airspace. Therefore, it seems that espionage in a national airspace of a state could be viewed as infringement of territorial sovereignty.

Historically, since the dawn of early aviation, states have recognized that airspace above the national territory belongs to that nation. The 1902 Resolution on the Law of the Air, Article 7 states that "every State has rights over its airspace which are necessary for its protection and for the suppression of espionage."[73] Then, in 1913 the International Law Association adopted a Resolution on the Law of the Air, and again it was stated that "the right of every state to enact such prohibitions, restrictions and regulations as it may think proper in regard to the passage of aircraft through the airspace above its territory...."[74] Interestingly, even the first documents on air law mention espionage.

---

[70] Commander Scott, *supra* note 52, at 220.

[71] KISH, *supra* note 55, at 97.

[72] *Id.*

[73] *Id.*, at 98.

[74] *Id.*

According to Professor Kish, "It is particularly significant that already the first drafts on air law specify the prohibition of espionage in national airspace."[75]

Article 1 of the 1944 Convention on International Civil Aviation (also known as the 1944 Chicago Convention) states that a state has complete and exclusive sovereignty over the airspace above its territory.[76] Article 3 of the Chicago Convention states that "aircraft used in military....service shall be deemed to be state aircraft. No state aircraft....shall fly over the territory of another state....without authorization...."[77] Notwithstanding the language of the Chicago Convention, Hays Parks, a national security law expert, states that "Penetration of a state's airspace for purposes of collection of intelligence, while often vaguely characterized as a 'violation of international law,' more correctly may be regarded as a violation of the sovereignty of that state as recognized by international law."[78] This is important because it emphasizes the fact that international law does not prohibit espionage.

Perhaps the most illustrative incident of espionage over national airspace is the U-2 incident.[79] In 1960 a U-2 reconnaissance aircraft of the United States was downed by the Soviet Union while it was flying over its national airspace.[80] Then Soviet Foreign Minister Andrei Gromyko stated at the time that "the U-2 flight was an aggressive action

---

[75] *Id.*

[76] Convention on International Civil Aviation, 61 Stat. 1180, T.I.A.S. 1591, 15 U.N.T.S. 295, 3 Bevans 944 (1944), Article 1.

[77] *Id.*, at Article 3.

[78] Parks, *supra* note 12, at 439.

[79] For an in-depth discussion of the U-2 incident, *see in general* FRANCIS GARY POWERS, OPERATION OVERFLIGHT (1970); THE TRIAL OF THE U-2 (1960); Quincy Wright, *Legal Aspects of the U-2 Incident*, 54 AM. J. INT'L L. 836 (1960).

[80] Parks, *supra* note 12, at 439; KISH, *supra* note 55, at 100.

unheard of in peace time."[81] The Soviets claimed that such flight was a *per se* act of aggression.[82] In response, President Eisenhower stated that the flights "had no aggressive intent but rather were to assure the safety of the United States and the free world against surprise attack by a power which boasts of its ability to devastate the United States and other countries by missiles armed with atomic war heads."[83]

Nonetheless, the U-2 incident was not characterized by the United Nations as a violation of international law. As Hays Parks explains:

> The U-2 flight was characterized by the United Nations Security Council as a violation of Soviet airspace, but not as an illegal use of force contrary to Article 2(4) of the Charter of the United Nations. From the U-2 incident it may be concluded that intelligence gathering by aircraft does not constitute *per se* violation of international law by the originating state, but that the state whose airspace is penetrated may resort to reasonable use of force to defend its sovereignty against such entry – although use of force should be only as a last resort.[84]

3. Espionage on the High Seas

According to Professor Kish, "The common legal status of international spaces determines the permissibility of espionage on the high seas."[85] Freedom of the high seas is customary international law.[86] Historically, the principle that no state may claim sovereignty over the high seas has been recognized in major international law

---

[81] Wright, *supra* note 79, at 840.

[82] IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES 363 (1963).

[83] Wright, *supra* note 79, at 842.

[84] Parks, *supra* note 12, at 439.

[85] KISH, *supra* note 55, at 102. For an excellent background information regarding the law of international spaces regime, *see in general* JOHN KISH, THE LAW OF INTERNATIONAL SPACES (1973).

[86] KISH, *supra* note 55, at 102.

documents and transactions. The 1926 Resolution on the Laws of Maritime Jurisdiction stated in Article 13 that "no State may claim any right of sovereignty over any portion of the high seas or place any obstacle to the free and full use of the high seas."[87] The freedom of the high seas principle was adopted in other documents/instruments, like the 1927 Resolution on Navigation on the High Seas; Draft Articles on the Regime of the High Seas to the International Law Commission; and Final Report on the Law of the Sea by the International Law Commission.[88] Further, the freedom of the high seas was codified in the 1958 Geneva Convention on the High Seas and reaffirmed in the 1982 United Nations Convention on the Law of the Sea.[89]

The freedom of the high seas thus allows for nations to carry out reconnaissance. The method of reconnaissance includes ships, aircraft, and submarines. For many years the United States has carried out a successful submarine espionage program.[90] "The freedom of the high seas includes the right of reconnaissance by ships on the high seas, submarines in the subjacent waters, installations on the deep seabed, and aircraft in the subjacent airspace."[91] If such espionage is conducted near a coastal state, then some issues may arise. "Although international law does not forbid electronic reconnaissance from the high seas and does not empower the coastal state to interfere with foreign

---

[87] *Id.*

[88] *Id.*, at 103

[89] *Id.*

[90] *See generally,* SONTAG & DREW, *supra* note 7.

[91] KISH, *supra* note 55, at 109.

warships or aircraft engaged in it, such reconnaissance is likely to be resented by coastal states and to heighten international tensions."[92]

Indeed, there have been some incidents that show how international tensions can arise as a result of espionage on the high seas, but none of these incidents raises any doubt about the legality of espionage on the high seas. According to Hays Parks:

> The North Vietnamese attack on the U.S.S. Maddox in the Gulf of Tonkin in 1964, the Israeli attack on the U.S.S. Liberty in 1967, and the North Korean seizure of the U.S.S. Pueblo in 1968, were cases in which attacks of vessels took place on the high seas in order to deny intelligence collection rather than repudiation of the concepts expressed herein.[93]

Professor Kish concludes "Consequently, the international regime consolidates the permissibility of espionage on the high seas."[94]

4. Espionage in Space

Space is also considered an international space regime like the high seas and Antarctica.[95] "From the start of space exploration, the principle of the freedom of outer space has been generally recognized in customary international law."[96] It is clear that the practice of states negates the concept of territorial sovereignty over outer space.[97] Espionage and intelligence collection in outer space can be accomplished by different

---

[92] Oliver J. Lissitzyn, *Electronic Reconnaissance From the High Seas and International Law*, NAVAL WAR COLLEGE, VOLUME 61, at 569.

[93] Parks, *supra* note 12, at 438.

[94] KISH, *supra* note 55, at 109.

[95] *See generally,* KISH, THE LAW OF INTERNATIONAL SPACES, *supra* note 85.

[96] KISH, *supra* note 55, at 115.

[97] Id.

methods.[98] But, the "precise nature and degree to which satellites are utilized for intelligence gathering has not been acknowledged by any nation."[99] Like submarine espionage, the United States has maintained a successful space espionage program.[100]

Historically, the prohibition of sovereignty over outer space was recognized by the first documents in this area.[101] The 1960 Hamburg Conference of the International Law Association drafted a document regarding the legal status of outer space.[102] This document states in one of its articles that "outer space may not be subject to the sovereignty of any state."[103] Another important document is the 1962 Draft Code of Rules on Outer Space. Commentary to Article 2(5) of the Draft Code of Rules on Outer Space states that "The prohibition does not extend to surveillance or reconnaissance satellites, which may primarily serve military purposes, yet have the advantage that they contribute to an open world and so increase rather than diminish security."[104] The principle of negation of territorial sovereignty over outer space was reaffirmed in the 1963 Brussels Resolution on the Legal Regime of Outer Space and in the 1967 Treaty on

---

[98] Thomas C. Wingfield, *Legal Aspects of Offensive Information Operations in Space*, 9 USAFA J. LEG. STUD., 121, 123 (1998/1999).

[99] Parks, *supra* note 12, at 441.

[100] *See generally,* BURROWS, *supra* note 7.

[101] KISH, *supra* note 55, at 116.

[102] *Id.*

[103] *Id.*

[104] *Id.*

Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (the Outer Space Treaty).[105]

The Outer Space Treaty contains the words "peaceful uses of outer space."[106] These words, according to Hays Parks:

> [w]ere not intended to and do not limit the use of outer space for intelligence-gathering purposes. This conclusion is reached not only in reviewing the practice of nations, but also by analogy to maritime treaties. 'Peaceful use' is not a legal term of art, but merely a descriptive phrase. Just as the phrase is not intended to preclude the use of the high seas by warships (including for intelligence-gathering purposes), it does not preclude the use of outer space by intelligence-gathering satellites.[107]

Another author has stated that United States claims for space espionage is a necessity for military security.[108] "That is, we claim that the surveillance of the Soviet Union by our satellites is an essential precaution against surprise attack."[109] Professor Kish concludes regarding the Outer Space Treaty that "The freedom of outer space thus includes the freedom of reconnaissance, especially, and most significantly, the strategic observation of national territory from outer space."[110]

---

[105] *Id.* at 117; *See also*, Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, 18 U.S.T. 2411, T.I.A.S. No. 6347, 610 U.N.T.S. 205 (1967).

[106] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, *supra* note 105.

[107] Parks, *supra* note 12, at 441.

[108] Richard A. Faulk, *Space Espionage and World Order: A Consideration of the Samos-Midas Program, in* ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW 55 (Roland J. Starnger ed., 1962).

[109] *Id.*

[110] KISH, *supra* note 55, at 117.

In general, regarding espionage in outer space, Professor Kish states:

> The freedom of outer space has ensured the establishment of a significant system of strategic observation. The surveillance of national territory from outer space facilitates the verification of compliance with agreements on arms limitations....Consequently, the regime of reconnaissance manifests the permissibility of espionage in outer space.[111]

B. Espionage Under Armed Conflict

Espionage, in time of war, "is a legitimate belligerent operation and is not a violation of the laws of war."[112] The main justification or rationale is that "war cannot be waged without all kinds of information about the forces and the intentions of the enemy, and about the character of the country within the zone of military operations."[113] Further, "While in the law of peace the territorial division of the regulation is based on the distinction between national spaces and international spaces, war transcends this distinction, and the territorial division of the regulation follows the main areas of hostilities: land, sea and air."[114] The laws of war's rules on espionage are "unique, clear and consistent."[115] According to Lauterpacht's edition of Oppenheim, "To obtain the necessary information, it has always been considered lawful to employ spies, and also to make use of the treason of enemy soldiers...."[116]

---

[111] KISH, *supra* note 55, at 120.

[112] ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW, *supra* note 19, at 114.

[113] OPPENHEIM'S, *supra* note 53, §159, at 422.

[114] KISH, *supra* note 55, at 123.

[115] Lt Col Geoffrey B. Demarest, *Espionage in International Law*, 24 DENV. J. INT'L L. & POL'Y 321, 330 (1996).

[116] OPPENHEIM'S, *supra* note 53, §159, at 422.

The above analysis does not end the discussion about espionage during armed conflict. Although international law does not prohibit espionage during armed conflict, there are other factors that come into play depending where and how espionage is conducted. To that end, espionage during wartime must be understood and analyzed according to location and method: (1) land warfare; (2) naval warfare; (3) air warfare; and (4) war spies. This analysis of espionage during armed conflict according to location and method will facilitate our study of espionage in cyberspace. Cyberspace could be viewed as a fifth "location and or method" where espionage during wartime is carried out.

1. Espionage in Land Warfare

The development of land warfare has historically confirmed the permissibility of espionage in land warfare.[117] Hugo Grotius, in his De Jure Belli Ac Pacis, states that sending "spies....is beyond doubt permitted by the law of nations – such as spies whom Moses sent out, or Joshua himself...."[118] Even though Grotius' comment is more than three centuries old, it is true today.[119] The Lieber Code recognized that espionage by belligerent states was permissible.[120] In 1874, the Declaration of Brussels Concerning the Laws and Customs of War, the Russian draft document followed the Lieber Code

---

[117] KISH, *supra* note 55, at 123.

[118] HUGO GROTIUS, DE JURE BELLI AC PACIS, Book III, Ch. IV xviii 655 (F. Kelsey translation, Oxford, 1925).

[119] Demarest, *supra* note 115, at 331.

[120] Instructions for the Government of the Armies of the United States in the Field, prepared by Francis Lieber, promulgated as General Orders No. 100 by President Lincoln, 24 April 1863, Adjutant Generals' Office, 1863, Washington 1898 [Lieber Code].

principles.[121] Article 13 of the Brussels Declaration states that "amongst the means of warfare which are permitted are the employment of every available means of procuring information about the enemy and the country."[122] According to Professor Kish, "the consistency of the American and the Russian attitudes to espionage indicated an evolving consensus in customary international law."[123]

In 1880, the Institute of International Law adopted the Manual of the Laws of War on Land which reaffirmed the principles regarding espionage in war.[124] In 1899, an international conference on the law of war was held at The Hague and reaffirmed espionage during war. Subsequently, the fruits of this conference resulted in the Convention and annexed Regulations on the Laws and Customs of War on Land. "With the entry into force of the Convention and the Regulations in 1900, the first multilateral conventional regulation of the law of war, including espionage, was accomplished."[125] The 1907 Hague Convention reaffirmed the permissibility of espionage in war.[126]

2. Espionage in Naval Warfare

According to Lauterpacht's edition of Oppenheim, "espionage and war treason do not play so large a part in sea warfare as in land warfare; but they may be employed."[127]

---

[121] KISH, *supra* note 55, at 123.

[122] *Id.*

[123] *Id.*

[124] *Id.*, at 124.

[125] *Id.*

[126] Hague Convention IV Respecting the Laws and Customs of War on Land, *reprinted in* ADAM ROBERTS & RICHARD GUELFF, DOCUMENTS ON THE LAWS OF WAR 78 (3rd ed 2000).

The basic principles of the law of war on land are also recognized at sea. The unique issue in naval warfare is neutral waters.[128] In 1907, the Hague Conference adopted a regulation concerning neutrality at sea.[129] This convention "attempts to harmonize the sensitive naval interests of neutral and belligerent States."[130] Basically, under this Convention, a belligerent can engage in surveillance while passing through neutral waters. Thus, "belligerent espionage is restricted, but not prohibited, in neutral waters."[131]

The legal scope of espionage in war at sea is explained by Professor Kish:

> The regulation of espionage by the international law of naval warfare reflects the distinction between the regimes of belligerency and neutrality. Although individuals engaged in clandestine surveillance at sea are considered war spies, the tactical importance of observation necessitates the belligerent state practice of naval reconnaissance. In contrast, neutral waters and neutral ships must not be used for the transmission of intelligence to the belligerents. Nevertheless, while belligerent ships passing through neutral waters may carry out observation of the enemy, neutral states are entitled to survey such passage...."[132]

3. Espionage in Air Warfare

The basic rule of espionage in air warfare is that "conventional and customary international law manifest the permissibility of reconnaissance during aerial warfare."[133]

---

[127] OPPENHEIM'S, *supra* note 53, §210, at 509.

[128] KISH, *supra* note 55, at 128.

[129] Hague Convention (XIII) Respecting the Rights and Duties of Neutral Powers in Naval War (18 October1907), *reprinted in* DIETRICH SCHINDLER & JIRI TOMAN, EDS, THE LAWS OF ARMED CONFLICT 941 (1988).

[130] KISH, *supra* note 55, at 128.

[131] *Id.*, at 129.

[132] *Id.*, at 133.

According to Professor Kish, "War transcends the peace-time distinction between the sovereignty of the subjacent state over national airspace and the jurisdiction of the flag state in international airspace, and belligerents may conduct hostilities both in the airspace above national territory....and in the airspace of the high seas."[134]

The 1899 Hague Convention on the Laws and Customs of War on Land extended its scope to aerial espionage.[135] The 1907 Hague Convention on the Laws and Customs of War reaffirmed the 1899 convention. Basically, the 1899 and 1907 Hague Conventions state that airmen carrying out their mission in the open are not spies. On the other hand, if airmen carry out their mission clandestinely, then they can be considered spies.[136] The Institute of International Law, in 1911, created a Draft Convention on the Juridical Regime of Aircraft.[137] According to Professor Kish, "Article 7 of the Draft Convention restricts the definition of espionage in aerial war to clandestine operations."[138]

Professor Kish summarizes the current rules on espionage in air warfare:

> The rules of belligerency and neutrality divide the international law of aerial warfare. Considering the military importance of aerial surveillance during hostilities, belligerent states are entitled to carry out such activities, while the individual responsibility of their airmen as war spies depends on the secrecy of their operations.

---

[133] *Id.*, at 134.

[134] *Id.*

[135] *Id.*

[136] Hague Convention (II) With Respect to the Laws and Customs of War on Land, Article 29, The Hague (July 29, 1899), *reprinted in* DIETRICH SCHINDLER AND JIRI TOMAN, THE LAWS OF ARMED CONFLICT (1988), at 63; Hague Convention and Regulations on the Laws and Customs of War on Land, Article 29, The Hague (October 18, 1907), *reprinted in* DIETRICH SCHINDLER AND JIRI TOMAN, THE LAWS OF ARMED CONFLICT (1988), AT 63.

[137] KISH, *supra* note 55, at 135.

[138] *Id.*

> The status of neutrality imposes further restrictions on aerial observation. For the protection of belligerent security, the prohibition of reconnaissance extends both to neutral airspace and to neutral aircraft.[139]

C. War Spies

The legal regime affords certain protection and sanctions to spies during armed conflict. The definition of a spy is "someone who, while in territory under enemy control or the zone of operations of a belligerent force, seeks to obtain information while operating under a false claim of noncombatant or friendly forces status with the intention of passing that information to an opposing belligerent."[140]

A spy does not commit an international crime,[141] or a war crime.[142] If captured wearing a uniform, he will be treated as a 'scout' and not as a spy.[143] If captured without uniform, then he cannot be punished without a trial.[144] Yet, "because of the danger it presents to national security, belligerents are entitled to punish spies as they see fit."[145] If the spy returns to his army and then later on is captured by the enemy, he is to be treated

---

[139] *Id.*, at 136.

[140] ANNOTATED SUPPLEMENT TO THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS, UNITED STATES NAVAL WAR COLLEGE (1997), at 12.8. *See also*, Lieber Code, Article 88(1); 1907 Hague Convention IV: Regulations Respecting the Laws and Customs of War on Land, Article 29; United States Uniform Code of Military Justice, Article 106; INTERNATIONAL LAW – THE CONDUCT OF ARMED CONFLICT AND AIR OPERATIONS, Chapter 9 (1976); THE LAW OF LAND WARFARE, UNITED STATES ARMY, Article 75 (1956).

[141] Richard Baxter, *So-Called 'Unprivileged Belligerency': Spies, Guerillas, and Saboteurs*, 1951 BRIT. Y.B. INT'L L. 333.

[142] GEORG SCHWARZENBERGER, A MANUAL OF INTERNATIONAL LAW 210 (5th ed., 1967).

[143] Ingrid Delupis, *Foreign Warships and Immunity For Espionage*, 78 AM. J. INT'L L. 53, 67 (1984).

[144] Hague Conventions on Land Warfare of 1899 and 1907, *supra* note 136, at Article 30.

[145] SCHWARZENBERGER, *supra* note 142, at 210.

as a prisoner of war.[146] If the spy is captured before joining his army, he is not entitled to prisoner of war status.[147]

The 1977 Protocols[148] to the 1949 Geneva Conventions[149] makes a distinction between spies and members "of armed forces who gather information in occupied territory where they are residents."[150]

IV. Basic Definitions of Cyber Terms

Operations in cyberspace have led to the creation and use of various terms. The purpose of this section is to clarify certain terms that will be useful in our analogies. In order to understand how espionage under international law is applicable in cyberspace, we must have a basic understanding of the terms applicable to cyberspace and warfare.

---

[146] Hague Conventions on Land Warfare of 1899 and 1907, *supra* note 136, at Article 31.

[147] INGRID DETTER, THE LAW OF WAR 148 (2000).

[148] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), *reprinted in* INTERNATIONAL COMMITTEE OF THE RED CROSS, COMMENTARY ON THE ADDITIONAL PROTOCOLS (1987).

[149] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, opened for signature 12 August 1949, entered into force 21 October 1950, 75 U.N.T.S. 31 (hereinafter Geneva GWS); Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, opened for signature 12 August 1949, entered into force 21 October 1950, 75 U.N.T.S. 85 (hereinafter Geneva GWS Sea); Geneva Convention Relative to the Treatment of Prisoners of War, opened for signature 12 August 1949, entered into force 21 October 1950, 75 U.N.T.S. 135 (hereinafter Geneva GPW); Geneva Convention Relative to the Protection of Civilian Persons in Time of War, opened for signature 12 August 1949 entered into force 21 October 1950, 75 U.N.T.S. 287 (hereinafter Geneva GC) *reprinted in* ADAMS ROBERTS & RICHARD GUELFF, DOCUMENTS ON THE LAWS OF WAR (3rd edition 2000).

[150] DETTER, *supra* note 147, at 148.

A. Information Operations

According to Department of Defense (DOD) Joint Publication (Joint Pub) 3-13, information operations are "actions taken to affect adversary information and information systems while defending one's own information and information systems. Also called IO."[151] Information operations is the umbrella term which all other cyber actions (either offensive or defensive) falls under. Information operations can be defensive or offensive.[152] Defensive information operations are the "integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend information systems."[153] Offensive information operations are "the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decision makers to achieve or promote specific objectives."[154]

B. Information Warfare

Information warfare is a sub-set of information operations. Thus, information warfare is "information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. Also called

---

[151] DEPARTMENT OF DEFENSE, JOINT PUB 3-13, JOINT DOCTRINE FOR INFORMATION OPERATIONS GL-7 (9 October 1998).

[152] *Id.*

[153] *Id.*, at GL-5.

[154] *Id.*, at GL-9.

IW."[155] In other words, information warfare is the area where the laws of war are most relevant. This also is the term most recognized and used by the public and media.[156]

C. Cyberwar

According to a Rand Corporation study on information warfare, cyberwar is explained as follows:

> Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting if not destroying the information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to 'know' itself: who it is, where it is, what it can do when, why it is fighting, which threats to counter first, etc. It means trying to know all about an adversary while keeping it from knowing much about oneself.[157]

It appears that the definition of cyberwar is similar to information warfare. Cyberwar is how the non-military organizations refer to warfare in cyberspace. Military organizations tend to refer to warfare in cyberspace as information operations or information warfare.

---

[155] *Id.*, at GL-7-8.

[156] For a general overview of information warfare, *see generally*, DENNING, *supra* note 26; SCHWARTAU, CYBERSHOCK, *supra* note 27; SCHWARTAU, INFORMATION WARFARE, *supra* note 27; INFOWAR (Gerfried Stocker & Christine Schopf eds., 1998); CYBERWAR (Alan Campen et. al. eds., 1996); CYBERWAR 2.0 (Alan Campen & Douglas Dearth eds., 1998); JAMES ADAMS, THE NEXT WORLD WAR (1998); THE FIRST INFORMATION WAR (Alan Campen ed., 1992); JEAN GUISNEL, CYBERWARS (1999).

[157] JOHN ARQUILLA & DAVID RONFELDT, CYBERWAR IS COMING! 6 (1992).

D. Netwar

The Rand Corporation defines netwar as follows:

> Netwar refers to information-related conflict at a grand level between nations or societies. It means trying to disrupt, damage, or modify what a target population "knows" or thinks it knows about itself and the world around it. A netwar may focus on public or elite opinion, or more likely, both. It may involve public diplomacy measures, propaganda and psychological campaigns, political and cultural subversion, deception of or interference with local media, and efforts to promote a dissent or opposition movements across computer networks.[158]

Netwar most likely will be carried out by a society – civilians. This is the situation at the present time between Israeli civilians and Palestinians and other terrorist groups.[159] The danger of netwar is that it can easily spill over the territorial boundaries of the parties engaged in such cyber attacks. Some of the attacks from the Palestinians have been directed at United States targets.

E. Cyberterrorism

According to Dorothy Denning, Professor at Georgetown University:

> Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical

---

[158] *Id.*, at 5.

[159] Gwen Ackerman, *A Virtual War*, THE JERUSALEM POST, November 5, 2000.

> infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.[160]

Depending on the conflict, a cyberterrorist attack could be a violation of the laws of war. Although this paper is not on cyberterrorism, it is important to understand the distinction between espionage and terrorism in cyberspace.

F. Computer Network Espionage (CNE)

Computer Network Espionage (CNE) is "the use of computers to gather intelligence against an adversary from his own system."[161] "It is the act through the medium of cyberspace of obtaining, transmitting, communicating, or receiving information about the national defense of a state with an intent, or reason to believe, that the information may be used to the injury of that state or to the advantage of any foreign nation."[162] Computer network espionage can be considered as a sub-set of information operations. Most importantly, computer network espionage should be distinguished and differentiated from a computer network attack.

G. Computer Network Attack

Computer Network Attack (CNA) is "Operations that disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and

---

[160] Dorothy Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, available at* http://www.terrorism.com/documents/denning-infoterrorism.html.

[161] WINGFIELD, *supra* note 65, at 349.

[162] *Id.*, at 374.

networks themselves."[163] According to the Department of Defense Joint Publication 3-13, CNA is a sub-section of information operations.[164]

The cyber terms defined above show something important about how we analogize current ideas and concepts into cyberspace. For example, in the physical world we have "terrorism", while in cyberspace we have "cyberterrorism". In the physical world we have air warfare, land warfare, and naval warfare. In cyberspace, then we have "cyberwar" or "information warfare". In the physical world we have "attacks," in cyberspace we have "cyberattacks." In the physical world we have espionage, in cyberspace then we should have "cyberespionage." This same method of analogy can be used when we think about "physical" status of espionage under international law. We can analogize such laws into cyberspace without creating new laws or regulations of espionage, and thus follow Judge Easterbrook's approach of the Law of the Horse, as it will be discussed below.

V. Old Wine Into New Wineskins?

Cyberspace. According to the United States Supreme Court, "the Internet is an international network of interconnected computers....Taken together, these tools constitute a unique medium -- known to its users as 'cyberspace' -- located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet."[165] This has been the challenge that cyberspace has presented to

---

[163] DEPARTMENT OF DEFENSE, JOINT PUB 3-13, *supra* note 151, at GL-5. *See also* WINGFIELD, *supra* note 65 at 374.

[164] *See generally,* DEPARTMENT OF DEFENSE, JOINT PUB 3-13, *supra* note 151.

[165] Reno v. ACLU, 521 U.S. 844, 117 S.Ct. 2329 (June 26,1997).

judges, scholars, and lawyers – where exactly is cyberspace and what is the jurisprudence that applies in this medium. According to a recently published book on the subject:

> The term "cyberspace" is a new one, coined by the science-fiction novelist William Gibson. As used in his "cyberpunk" fiction (a genre more-or-less invented by him with his novel Neuromancer) the term refers to what he calls a "consensual hallucination" which futuristic computer network users experience when "jacking-in" to a world-wide computer network. However, the term has come into popular usage as a name for the Internet. This term need not be confined simply to networks. If cyberspace is considered to apply to all phenomena occurring electronically "within" computers, the term's usefulness as a general descriptive term is clear. *The question remains open: is cyberspace an existence or an occurrence at all or is it something quite unique?*[166]

The question posed above bears directly on the discussion whether cyberspace is something "unique," thus requiring new laws, or whether cyberspace is old wine in new wineskins, thus requiring no new laws, but applications of old principles into new situations. This question also serves as the catalyst for the on-going discussion regarding cyberspace and the law. There are two primary camps on this discussion. Professor Lessig leads one school of thought; the other is led by Judge Easterbrook.

A. Lessig's *Code*

Professor Lessig's basic position is that a "law of cyberspace" could teach lawyers, judges, and scholars something about the law.[167] He believes that cyberspace should be regulated. He describes four modalities of cyberspace regulation. The fourth mode – architecture – "or its code, regulates behavior in cyberspace. The code or the

---

[166] DAVID R. KOEPSELL, THE ONTOLOGY OF CYBERSPACE 11 (2000) (emphasis on the cite are mine).

[167] Lessig, *The Law of the Horse, supra* note 14, at 1.

software and hardware that make cyberspace law the way it is, constitutes a set of constraints on how one can behave."[168] In other words, cyberspace is unique and it presents special problems for the law. It should be regulated.

In one example explained by Professor Lessig, he demonstrates how cyberspace is unique and presents special problems for the law. He presents the problem of minors buying pornographic materials. In physical space, the store attendant selling those products can identify when a minor is attempting to buy an adult magazine and will refuse to sell it. In cyberspace, the "web site" cannot identify the minor, and thus an illegal sale will be made.[169] This is the problem of anonymity created by cyberspace, and just one example of many.

B. Judge Easterbrook's *Law of the Horse*

On the other hand, Judge Easterbrook explains that cyberspace is not unique when dealing with the law.[170] Cyberspace is a phenomenon like other phenomena or challenges that the law has faced before. Specifically, he explains:

> "....the best way to learn the law applicable to specialized endeavors is to study general rules. Lots of cases deal with people kicked by horses; still more deal with the licensing and racing of horses, or with the care veterinarians give to horses, or with prizes at horse shows. Any efforts to collect these strands into a course on "The Law of the Horse" is doomed to be shallow and to miss unifying principles. Teaching 100 percent of the cases on people kicked by horses will not convey the law of torts very well. Far better for students....for those who plan to go into the horse trade – to take courses in

---

[168] *Id.*, at 5.

[169] *See generally, id.*

[170] Easterbrook, *supra* note 15, at 1.

> property, torts, commercial transactions....Only by putting the law of the horse in the context of broader rules about commercial endeavors could one really understand the law about horses....When asked to talk about 'Property in Cyberspace,' my immediate reaction was, 'Isn't this just the law of the horse?'"[171]

The present status of espionage under international law should not require any new treaties or regulations for it to apply in or through cyberspace. Professor Lessig's approach to more regulation of cyberspace is not necessarily the answer. For one scholar, "Lawrence Lessig's *Code and Other Laws of Cyberspace*....excellently summarizes the current state of Internet law. However, his calls for more legislation and increased regulation of this medium are not backed by a sound ontology which would distinguish this medium from any other."[172] Judge Easterbrook's approach appears more reasonable and logical – at least in the area of espionage. Under Judge Easterbrook's approach, there should not be a "cyberlaw of espionage." The present status of espionage under international law should apply in cyberspace.

Applying these two schools to the current status of espionage under international law, the question arises whether new treaties, protocols, or other regulations are needed specifically for cyberspace. Or, is the current status of espionage under international law applicable to cyberspace? To illustrate the point, when the tank was invented, a "law of the tank" was not created. Thus, obviously, the application of technological advancement in the military to current law does not necessarily require the creation of new law in order to fit such advances within the context of present law. Accordingly,

> When only some of the consequences of new technologies,

---

[171] *Id.*

[172] KOEPSELL, *supra* note 166, at 17.

> however, fall beyond the defined parameters of acceptable activity, as was the case with aerial bombardment, *the new means and methods of warfare are simply regulated by existing law*, and when necessary, treaty law and evolving state practice.[173]

Although there is no question that cyberspace has brought confusion and possibly some chaos to certain areas of the law, specifically in the area of intellectual property,[174] it does not mean that all previous notions and principles of law are not valid in cyberspace. Accordingly, "The rise of an electronic medium that disregards geographical boundaries throws the law into disarray by creating entirely new phenomena that need to become the subject of clear legal rules, but that cannot be governed, satisfactorily, by any current territorially based sovereign."[175]

In addition to using Judge Easterbrook's approach, the use of analogies can be of assistance in our task. Many courts have relied on analogies when dealing with and resolving issues of law and cyberspace. For example, in American Libraries Association v. Pataki, the court explains the use of analogy to solve the issues related to cyberspace and law:

> The Internet may well be the premier technological innovation of the present age. Judges and legislators faced with adapting existing legal standards to the novel environment of cyberspace struggle with terms and concepts that the average American five-year-old tosses about with breezy familiarity. Not surprisingly, much of the legal analysis of Internet-related issues has focused on seeking a familiar analogy for the unfamiliar. Commentators

---

[173] WINGFIELD, *supra* note 65, at 5.

[174] *See generally,* KOEPSELL, *supra* note 166; LEMLEY, ET AL., *supra* note 13; David G. Post, *Governing Cyberspace, or Where is James Madison When We Need Him?,* PLUGGIN IN (June 1999); David Johnson & David Post, *And How Shall the Net Be Governed?, in* COORDINATING THE INTERNET (Brian Kabin & James Keller eds., 1997).

[175] David Johnson & David Post, *Law and Borders – The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

> reporting on the recent oral argument before the Supreme Court of the United States....noted that the Justices seemed bent on finding the appropriate analogy which would tie the Internet to some existing line of First Amendment jurisprudence: is the Internet more like a television? a radio? a newspaper?....This case, too, depends on the appropriate analogy. I find....that the Internet is analogous to a highway or railroad.[176]

Thus, analogies could be useful when explaining cyberspace and espionage. Other authors have resorted to analogies when dealing specifically with cyberspace. We could explain cyberespionage by analogizing it to space, airspace, sea, and land espionage. Cyberespionage could thus be explained as the intersection of either, space, airspace, sea, or land espionage at the cyberspace level.

VI. Application of Current Status of Espionage Under International Law in Cyberspace

According to the United States Army Operations Law Handbook, regarding information operations:

> In the array of challenges that face an operational attorney today, there is perhaps no more misunderstood, misapplied, mysterious task than that of coordinating the legal aspects of information operations (IO). The debate whether IO add a new dimension to our warfighting capability or represent a revolution that will reshape the way the Army accomplishes its strategic objectives remain unsettled.[177]

The following analysis is intended to answer the question: is the present status of espionage under international law applicable in or through cyberspace? But the analysis is also intended to pierce the veil of fog identified in the United States Army Operational Law Handbook in this area.

---

[176] American Libraries Association v. Pataki, 969 F.Supp 160 (1997).

[177] United States Army Judge Advocate General's School, OPERATIONAL LAW HANDBOOK at 25-1 (2000).

A. Cyberespionage During Peacetime

As we have discussed above, physical espionage in national territory is not prohibited by international law, but if the spy is captured, then he can be prosecuted under the domestic laws of the targeted nation. In cyberspace, the same rationale should apply. The act of spying remains the same. Cyberspace is not unique in this respect.

There have been some proposals to control information warfare and espionage in cyberspace. These proposals could affect the existing rules and status of espionage in cyberspace.

One proposal has appeared in a law review article. The author proposes that "international law must redefine its definition of espionage to account for the dangerous combination of potential harm and unaccountability that IW [information warfare] presents."[178] The proposition is based on the fact that cyberespionage "attacks" can be carried out many hundreds or thousands of times more in a single day than physical espionage.[179]

In another proposal, as indicated previously, the Russians have recommended restrictions on information warfare.[180] The proposal "calls upon Members States to promote at multilateral levels the consideration of existing and potential threats in the field of information security."[181]

---

[178] Michael Robbat, *Resolving the Legal Issues Concerning the Use of Information Warfare in the International Forum*, 6 B.U. J. SCI. & TECH. L. 10, at paragraph 49.

[179] *Id.*

[180] DOD OFFICE OF GENERAL COUNSEL, *supra* note 41, at 53.

[181] U.N. Doc A/RES/53/70 (1999).

Under the Lessig approach, there should be new laws regulating espionage in cyberspace. In this respect, the argument would be that espionage in cyberspace needs regulation like other areas of the law, for example intellectual property in cyberspace. The argument could be extended that failure to create new rules for espionage in cyberspace could bring confusion in certain areas of the law just like the cyberspace technology of Napster[182] has brought chaos to the intellectual property laws.

Another argument that supports the Lessig approach is how governments have dealt with criminal law in cyberspace.[183] At the present time, the United States and many other nations have passed legislation creating cyber crimes.[184] When computer hackers began to invade and trespass into other people's computers, including government computers, governments realized they did not have laws to prosecute those cyber crimes.[185] The European Council even drafted a treaty to deal with computer crimes at the international level.[186]

Under the Easterbrook approach, there is or there should be one legal regime of espionage, to include cyberspace. The rationale would be that the present rules or

---

[182] According to Computer User High-Tech Dictionary, it describes Napster as "Dot-com offering MP3 downloads, filesharing and online community resources. The Recording Industry Association of America, as well as recording artist Dr. Dre and the heavy metal group Metallica, sued Napster in early 2000 for promoting unlawful trade of copyrighted music. Judges have threatened to shut Napster down, and currently the future of the site is still in the hands of the court." *Available at* http://www.computeruser.com/resources/dictionary/

[183] *See generally,* ULRICH SIEBER, THE INTERNATIONAL EMERGENCE OF CRIMINAL INFORMATION LAW (1992).

[184] *E.g.,* 10 U.S.C.A. § 1030 (West 2000) , makes computer hacking under certain circumstances a crime. *See in general*, DAVID ICOVE, KARL SEGER & WILLIAM VONSTORCH, COMPUTER CRIME (1995).

[185] *See in general* the interesting story of Cliff Stoll attempt to catch a cyber criminal/spy and the challenges he faced when at the time governments were beginning to realize the threat of computer crimes to society. CLIFF STOLL, THE CUCKOO'S EGG (1989).

[186] *See generally,* Council of Europe, *Draft Convention on Cyber-crime* (Draft No 25 REV. 5), *supra* note 45, *available at* http://conventions.coe.int/treaty/EN/cadreprojets.htm.

principles governing espionage in international law then should be applied to cyberespionage. Where the present legal regime of espionage allows for total permissibility to spy on other countries, for example espionage in international spaces, then the same current principles should apply to espionage in cyberspace. Thus, cyberespionage in national territory should be considered and treated the same way as the present rules of "physical" espionage in national territory.

Applying the Easterbrook approach then, a strong argument can be made, that there is no need to create new rules or laws to regulate cyberespionage over or through national territory. The present status of espionage over national territory should apply to espionage in cyberspace. Therefore, based on the current status of espionage over national territory, espionage in cyberspace that actually touches national territory could be considered a crime under the domestic laws of the targeted country, but not a violation of international law. The principle of "*tu quoque*" then should be the guiding principle of international law for cyberespionage that is conducted in national territory of another country.

Yet, there is another possible argument of the legality of cyberespionage under international law. National security law expert, Thomas C. Wingfield, opines that there are presently certain methods of collecting intelligence that could be considered as transpiring in cyberspace and that are not prohibited by international law.[187] The methods he identifies as transpiring in cyberspace are: SIGNIT,[188] COMINT,[189]

---

[187] WINGFIELD, *supra* note 65, at 350. .

[188] Signals intelligence.

[189] Communications intelligence.

ELINT,[190] FISINT,[191] and IMINT.[192] Assuming that these methods of espionage do not transpire in cyberspace, we could analogize them to the internet or cyberspace. We could argue that since these methods of espionage are not prohibited by international law, espionage in cyberspace should not be prohibited either.

Because customary international law recognizes that territorial sovereignty also extends to national airspace above national territory, the same analysis and conclusions as above should apply to cyberespionage in national airspace. One method of carrying out cyberespionage in national airspace could be through wireless internet access and/or PalmPilots, or Personal Digital Assistants.[193] Therefore, under the Easterbrook approach cyberspace espionage over national territory should be treated as traditional physical espionage over national territory. As with the U-2 overflight incident, the targeted nation could resort to certain defenses.

Cyberespionage on the high seas should not confront any major criticism or prohibition because (however it could be done – cyberespionage on the high seas) of the customary international law of freedom of the high seas. Because no state can claim sovereignty over the high seas, no state can claim a violation of its territorial integrity.

Regarding cyberspace espionage in outer space, it should also not face any major criticisms or prohibitions because space is considered an international space like the high seas and Antarctica. "Two of the newest ways to connect to the Internet and browse the

---

[190] Electronic intelligence.

[191] Foreign instrumentation signals intelligence.

[192] Imagery intelligence.

[193] "Personal Digital Assistants can literally put the Web in the palm of your hand." PRESTON GRALLA, HOW THE INTERNET WORKS 75 (1999).

Web are via satellite connections...."[194] The only challenge of cyberespionage in outer space via satellites is the possibility of violating one of the present international agreements covering satellite communications.[195]

B. Cyberespionage During Armed Conflict

A news report titled "Pentagon Dubs Cyberspace As Key Battlefield," stated that "the Defense Department....revealed its plan for how the military services will carry out offensive and defensive information operations in future wars – a move that holds wide-ranging implications for information systems."[196] Further, according to General Henry Shelton[197] such information operations plan "includes both offensive and defensive information warfare operations, [that are] as crucial to the national defense as air, land or naval operations."[198] The National Security Agency will support this information operations plan.[199] Intelligence collection, espionage, and reconnaissance are part of any military operation, especially during armed conflict. Therefore, it appears that cyberspace itself could be an actual battlefield. This is what is being called a "cyberwar"

---

[194] *Id.*

[195] *E.g.*, Agreement Relating to the International Telecommunications Satellite Organization, June 29,1971, 23 U.S.T. 3813, T.I.A.S. No. 7532 (INTELSAT); Convention at the International Maritime Satellite Organization, 3 Sept. 1976, 31 U.S.T. 1, T.I.A.S. No. 7532 (INMARSAT); International Telecommunications Conventions of 1982, 6 Nov. 1982 (Nairobi Convention).

[196] Bob Brewin & Daniel Verton, *Pentagon Dubs Cyberspace As Key Battlefield*, FEDERAL COMPUTER WEEK, 7 December 1998, *at* http://208.201.97.5/pubs/fcw/1998/1207/fcw-newscyber-12-7-98.html

[197] The present Chairman of the Joint Chiefs of Staff, Department of Defense.

[198] Brewin & Verton, *supra* note 196, *at* http://208.201.97.5/pubs/fcw/1998/1207/fcw-newscyber-12-7-98.html

[199] *Id.*

or sometimes "netwar". Cyberespionage, then could take place not only during physical armed conflict, but also during information operations proper.

Unlike espionage during peacetime, espionage during wartime is not limited by territorial sovereignty. The only limiting factor of espionage during wartime is regarding the issue of neutral states. Applying the Lessig approach does not make sense. There should not be any new regulations prohibiting or limiting cyberespionage during armed conflict. Espionage is permissible during armed conflict, while during peacetime it is subject to territorial sovereignty. It does not make sense to regulate or create new laws of an activity that is accepted by nations during wartime.

On the other hand, under the Easterbrook approach, cyberespionage during land warfare, naval warfare, air warfare, and space warfare does not represent a problem. The principles applicable to current espionage during armed conflict should also apply in cyberspace. Espionage in cyberspace during armed conflict could be interpreted as an extension of physical espionage.

Also, by analogy we can understand and accept espionage in cyberspace as a continuation and development of previous forms of espionage. An armed conflict two hundred years ago would rely on traditional human espionage. World War I saw the emergence of the airplane as an intelligence collection platform. Submarine espionage was used during WWI and WWII. The invention of electronic devices allowed for better and more intrusive forms of espionage during armed conflict. Once satellites were put into orbit, they were used for intelligence collection. Now, cyberspace could be seen as yet another method of wartime espionage. All previous methods of espionage during

wartime were not prohibited. Therefore, cyberespionage during armed conflict should not be regulated by international agreements or new rules of international law, either.

C. War Spies in Cyberspace

The advantage of a war cyberspy is that he should not fear apprehension. Also, he can operate from almost anywhere in the world. Therefore, a cyberspy may not have to worry too much about being captured, opposite his brethren that actually go inside a country to spy. As noted in a recent news report titled "U.S. Army Kick-Starts Cyberwar Machine," "The Internet is ubiquitous. It allows attacks from anywhere in the world. Attackers can loop in from many different Internet providers, said....who noted that a cyberattack can include espionage using computer networks."[200]

The Department of Defense is presently engaged in a netwar and/or involved in a cyberterrorism battle in cyberspace.[201] Perhaps then it could be argued that the armed conflict rules for espionage in cyberspace should be applicable at the present time, what appears to be "peacetime." According to Rep. Curt Weldon, R-Pennsylvania, "There is an attack under way. You can basically say we are at war."[202] The perception may be that since we cannot "see" in physical space these cyberattacks, we may sense no urgency to carry out espionage in cyberspace as one of the tools to combat hostile computer hackers.

---

[200] Messmer, *supra* note 35, *at* http://www.nwfusion.com/news/2000/1120cyberattack.html?nf

[201] *Pentagon At War With Computer Hackers*, CNN, 5 March 1999, at http://www.CNN.com.

[202] *Id.*

VII. Consequence of Cyberespionage I: Computer Network Espionage As Armed Attack

As previously discussed, it appears that cyberespionage is legal and not prohibited by international law. However, cyberespionage, unlike physical espionage, could have serious consequences if the targeted country perceives such intrusion as an armed attack.[203] Under the United Nations Article 2(4), members have agreed to "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations."[204] Although it is beyond this paper to examine the question whether a computer network attack is an act of war or whether it constitutes use of force, we will briefly examine the issues involved in differentiating between computer network espionage and computer network attack.

A. Difficulty of Differentiating Between CNA and CNE

National security law expert, Thomas Wingfield, explains the consequences and difficulty of differentiating between CNA and CNE:

> The amount of damage done in pure collection activities is usually negligible, both because the intent is to gather intelligence and not inflict harm, and because any damage done, like a vase broken by a clumsy burglar, would be inadvertent and would serve to alert the target nation that it was being ransacked. Computer network attack, on the other hand, is an intentional use of force by definition. Any damage done in the real world, would serve, at the very least, as the basis for a colorable claim of use of force,

---

[203] For an excellent in-depth examination of this issue, see in general Michael Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885; SHARP, *supra* note 1; WINGFIELD, *supra* note 65; DOD OFFICE OF GENERAL COUNSEL, *supra* note 41; CYBERWAR: SECURITY, STRATEGY AND CONFLICT IN THE INFORMATION AGE (Alan D. Campen et al. eds. 1996); Campen, CYBERWAR 2.0, *supra* note 156.

[204] U.N. CHARTER article 2(4). *See also* DOD OFFICE OF GENERAL COUNSEL, *supra* note 41.

and possibly, an armed attack.[205]

Each nation may interpret such computer network intrusion differently. A nation may reserve the right to respond to an information warfare attack with a physical armed attack.[206]

B. Self-defense by Target Country

If the targeted country of computer network espionage perceives such intrusion as a computer network attack and as an armed attack, then such nation could claim a right of self-defense under Article 51 of the United Nations Charter.[207] The targeted country would have to show, first, that such computer network espionage is a computer network attack (CNA). Then, such country would have to show that such computer network attack is an "armed attack" under Article 2(4) and Article 51 of the United Nations Charter.[208] As Professor Schmitt describes in his seminal work, this is not an easy task.[209] Professor Michael Schmitt states:

> Since the Charter use of force prohibition reflects a fair degree of imprecision in the CNA context, this approach would favor greater inclusivity in gray area applications of the norm. This predilection to restrictions on CNA operations should not be interpreted as a suggestion that the criteria for armed attack be relaxed. On the contrary, maintaining a relatively high threshold for triggering the

---

[205] WINGFIELD, *supra* note 65, at 349.

[206] DOD OFFICE OF GENERAL COUNSEL (1st ed,1999), *supra* note 41, at 20.

[207] U.N. CHARTER article 51. *See also,* DOD OFFICE OF GENERAL COUNSEL, *supra* note 41, at Chapter III.

[208] For an excellent overview of responding to CNA against the United States' critical infrastructures, *see in general* Colonel James P. Terry, USMC (Ret), *Responding to Attacks on Critical Computer Infrastructure: What Targets? What Rules of Engagement?* 46 NAVAL L. REV. 170.

[209] Schmitt, *supra* note 203.

> right to respond to CNA in self-defense, although not enhancing its deterrent effect, serves to maintain constraints on the usually more disruptive act of unilateral resort to armed force.[210]

VIII. Consequence of Cybersespionage II: Criminal Liability for Cyberspies

As with physical espionage, a cyberspy may face criminal liability for his acts. The danger of prosecution exists in peacetime and wartime. As stated above, the criminal liability he faces is not for international crimes or war crimes, rather, the criminal liability is for breaches of domestic laws.[211]

A. Foreign Domestic Laws Against Espionage

Since a spy does not act against the law of nations, he cannot face a trial for an international crime. Rather, if captured, the spy can be prosecuted for a violation of the domestic laws of the targeted country.[212] Although "the employment of spies is no offense against the laws of war," [213] "espionage is, however, unlawful under the domestic law of most states during peacetime and armed conflict."[214] National security law expert, Hays Parks, elaborates, stating that "Spies are punished, not as violators of international law, but to render that method of obtaining information as dangerous, difficult, and ineffective as possible."[215] Regarding criminal liability for espionage during peacetime

---

[210] *Id.*, at 936.

[211] DOD OFFICE OF GENERAL COUNSEL, *supra* note 41, at 42.

[212] Parks, *supra* note 12, at 435.

[213] Henry Wager Halleck, *Military Espionage*, 5 AM. J. INT'L L. 593 (1911).

[214] WINGFIELD, *supra* note 65, at 350.

[215] Parks, *supra* note 12, at 435.

and wartime, "Spying in peacetime is a criminal offense against the domestic law of the targeted country; in wartime, the offense is the same, but the penalty usually is capital to serve as a further disincentive to spying."[216] In the recent news, the networks have devoted a vast amount of time to explain the punishment facing FBI Counterintelligence Agent Robert Hanssen, alleged to commit espionage for Russia.

B. Location of the Cyberspy

The main difference of a physical spy and a cyberspy is the "location." A spy that is conducting espionage in Country X, is physically there. If arrested, Country X officials have possession of him. He can then be incarcerated and then be tried under the domestic laws of Country X. The physical presence of the spy in Country X means that he can be seen – he is not anonymous.

On the other hand, a cyberspy in Country X is anonymous and his only presence is in cyberspace. Such cyberspy cannot be arrested or identified. Further, the place of the spy's physical operations may not be possible to identify.[217] Therefore, prosecution of a cyberspy is extremely difficult. According to the DOD Office of General Counsel:

> That leaves the issue of the possible criminal liability for an information operator who may later come into the custody of a nation that has been the victim of an operation in which he or she was engaged. As with a spy, there is no evident theoretical reason why such an individual could not be prosecuted for violation of the victim nation's criminal laws. As a practical matter, however, the problems of detection and attribution of information operations activities at the national level are daunting: the likelihood of being

---

[216] *Id.*

[217] With the present technology, a computer operator may appear to be physically in one country, when in fact, he may be located in another country.

> able to prove in court that an individual engaged in a certain information operations activity – while not impossible – seems small.[218]

Another law review article describes the situation:

> IW [information warfare] confounds the present framework, however, because it defies the metaphysical concept that an individual need be physically present in the target country in order to commit the act. Thus, even if the attack can be traced back to its source, the actor cannot legally be apprehended absent an extradition treaty. But no nation will extradite one of its own agents.[219]

IX. The Future of Cyberespionage

As we have seen in this paper, espionage has existed since time immemorial and it is not prohibited by international law. Humans, tribes, nations, and governments have resorted to espionage for many reasons and have used different methods of espionage. Espionage methods are varied. Technology allows for greater intrusion and penetration of a targeted country's secrets and information. What if there is a technology that could provide for absolute espionage and penetration into other computers by cracking encrypted information in a very fast manner? In other words, what if there is a computer capable of breaking all encryption programs? That could be the ultimate computer network espionage tool – and such technology is the quantum computer. The first nation capable of developing a quantum computer would be able to read any encrypted messages, access any bank account or military secret files – the perfect computer network espionage tool. The question would be, given its amazing implications, whether quantum cyberespionage would be legal under international law. In a recent national

---

[218] DOD OFFICE OF GENERAL COUNSEL, *supra* note 41, at 43.

[219] Robbat, *supra* note 178, at paragraph 48.

bestseller book, The Code Book: The Science of Secrecy From Ancient Egypt to Quantum Cryptography, the author's last line of the book asks "How would governments regulate quantum cryptography....?[220]

A. Quantum Computers, Cryptography, and Cyberespionage

Cryptography is "the art and science of scrambling information to keep a message secret. The better the cryptography, the better the secret is kept."[221] Cryptography is one of the most important technologies used to preserve our national security. "As far as the Department of Defense is concerned, cryptography and nuclear technology are two of the most sensitive areas in science and research since they both represent military strength."[222]

A technical description of how a quantum computer works is beyond this paper and for that matter beyond most legal literature.[223] In order to understand such technology, you will need a working knowledge of Einstein's Theory of Relativity and of quantum physics. But, in the most basic attempt to describe such technology, a quantum computer is "a computer that could, in theory, take seconds to perform calculations that

---

[220] Simon Singh, THE CODE BOOK: THE SCIENCE OF SECRECY FROM ANCIENT EGYPT TO QUANTUM CRYPTOGRAPHY 350 (1999).

[221] SCHWARTAU, INFORMATION WARFARE, *supra* note 27, at 232.

[222] *Id.*

[223] "Computation by computers using quantum-mechanical or DNA-biomolecular mechanisms to encode and store numerical symbols and perform computation will permit orders of magnitude increases in processing performance due to parallelism. Quantum computers encode symbols as a quantum bit or *qubit*, which can encode a linear superposition of two states (unlike the binary *bit* that encodes two possible states). Due to superposition and parallelism, the quantum computer can perform many functions exponentially faster than a conventional computer." EDWARD WALTZ, INFORMATION WARFARE: PRINCIPLES AND OPERATIONS 372 (1998).

would take today's fastest supercomputers longer than the age of the universe...."[224] Further, "quantum computers will be able to crack many of the leading methods of protecting secret information, while offering new unbreakable codes."[225] Therefore, as you can see, quantum computers will have an amazing and deep effect on cyberespionage and international law. A government possessing such technology would be able to perform effective and possibly limitless espionage in cyberspace.

Julian Brown, a science journalist, best describes the overall effect of quantum computers on cyberespionage and the international community:

> ....a quantum computer could far exceed the capabilities of a conventional computer....because of the huge repercussions such a machine would have for military communications, government secrecy and surveillance, data protection, e-commerce, and the privacy of ordinary citizens. If anyone could build a full-scale quantum computer, it's possible that he or she would be able to access everything from your bank account to the Pentagon's most secret files. It's no surprise, then, that significant funds backing this line of research have come from such organizations as the U.S. Department of Defense, the National Security Agency, NATO, and the European Union. If anybody is going to build one of these machines, the intelligence agencies are making certain they know about it first.[226]

B. What are the limits?

The limits are with the first government that can create or build a quantum computer. It appears, based on the information contained in this paper and the analyses, that international law will not prohibit quantum cyberespionage. The worst case scenario would be that, like nuclear weapons technology, if quantum computing technology is

---

[224] JULIAN BROWN, MINDS, MACHINES, AND THE MULTIVERSE: THE QUEST FOR THE QUANTUM COMPUTER, Introduction (2000).

[225] *Id.*, at introduction.

[226] *Id.*, at 25.

created or stolen by hostile governments, then quantum computing technology itself will be our only defense. An encrypted message using quantum technology cannot be broken.[227] But, it still would be a dangerous technology in the hands of a hostile government or group.

X. Conclusion

Espionage is an integral tool of nations. Intelligence collection and espionage has always been part of human history. Espionage during peacetime and wartime is regarded as a vital necessity in the national security process.

At the present time, there are no international law prohibitions against espionage during peacetime. Espionage is legal under international law during armed conflict. The current status of espionage under international law in peacetime and wartime is applicable in cyberspace. Therefore, there is no need to reinterpret espionage under international law in cyberspace. There is no need for new treaties to regulate or control espionage in cyberspace among nations. The argument has been raised that new laws or interpretations are needed to adapt certain areas of the law into cyberspace. On the other hand, the opposite argument is that there is no need for new laws – that current principles of laws can be analogized into cyberspace.

The methods to carry out espionage have changed throughout history. Nations have taken advantage of technological advances to improve their intelligence collection and espionage capabilities. First, it was simple physical surveillance espionage. Then, with the advent of electronic devices, electronic espionage was born. Following the

---

[227] SINGH, *supra* note 220, at 349.

invention of airplanes and submarines, nations resorted to aerial and submarine espionage. After space flights were possible, they resorted to space espionage. These types and methods of espionage and collection of intelligence are practiced by nations. Cyberespionage is just another espionage tool available to governments.

APPENDIX 1
OF THESIS

SUMMARY CHART

APPLICABILITY OF CURRENT STATUS OF ESPIONAGE UNDER INTERNATIONAL LAW INTO CYBERSPACE

Applicability of Current Status of Espionage Under International Law Into Cyberspace

Jorge H. Romero

Peacetime Espionage	Wartime Espionage	Cyberespionage	Treaty Law, Resolutions, Other International Law Documents
Basic Rules: * Principle of *"Tu Quoque"* * Not a violation of international law **National Territory** * No international law prohibition * Limitations: if spy is captured in target country, he is subject to domestic criminal laws of target country (but not for an international crime) **National Airspace** * No international law prohibition * Limitations: flights are subject to self-defense of targeted nation	**Basic Rules:** * Legitimate belligerent operation * Not a violation of the laws of armed conflict **Land Warfare** * No laws of war prohibition * Limitations: none **Air Warfare** * No laws of war prohibition * Limitations: adjacent neutral nations **Naval Warfare** * No laws of war prohibitions * Limitations: neutral waters	**Basic Rules:** **[by extrapolation and analogy to current status of espionage under international law]** * Principle of *"Tu Quoque"* * Not a violation of international law or laws of war **Peacetime** **National Territory** * Same principles and limitations as peacetime espionage **National Airspace** * Same principles and limitations as peacetime espionage	[some of these treaties and documents may not be applicable today; shown for historical analytical purposes] **Peacetime** **National Territory** * Charter of the UN * Convention on Diplomatic Relations **National Airspace** * 1902 Brussels Resolution on the Law of the Air * Paris Convention of 1919 * 1944 Chicago Convention * 1960 UN Security Council characterization of U-2 flight incident

High Seas
* No international law prohibition
* Limitations:
  - subject to self-defense of coastal state if naval platform is too close
  - no reconnaissance during innocent passage

Space
* No international law prohibition
* Limitations: none

War Spy
* No laws of war prohibitions
* Limitations: if captured, spy subject to domestic criminal laws of targeted country (but not for an international crime or war crime)

High Seas
* Same principles and limitations as peacetime espionage

Space
* Same principles and limitations as peacetime espionage

Wartime

Land Warfare
* Same principles and limitations as wartime espionage

Air Warfare
* Same principles and limitations as wartime espionage

Naval Warfare
* Same principles and limitations as wartime espionage

War Spy
* Same principles and limitations as wartime espionage

High Seas
* 1926 Resolution on the Laws of Maritime Jurisdiction
* 1927 Resolution on Navigation on the High Seas
* 1958 Convention on the High Seas
*1982 UNCLOS

Space
* 1960 Hamburg Resolution on the Legal Status of Outer Space
* 1962 Draft Code of Rules on Outer Space
* 1963 Brussels Resolution on the Legal Regime of Outer Space
* 1967 Treaty on Outer Space

Wartime

Land Warfare
* 1863 Lieber Code
* 1874 Brussels International Declaration on the Laws and Customs of War
* 1899 Hague Convention
* 1907 Hague Convention

Advantages:
* Cyberspy cannot be arrested in targeted country
* Anonymity
* Easier to claim plausible deniability

Disadvantages:
* Target country could misunderstand cyberespionage for a computer network attack

Limitations:
* Possible issues of Internet information "packets" traveling in cyberspace through a neutral country

Air Warfare
* 1899 Hague Convention
* 1911 Draft Convention on the Juridical Regime of Aircraft
* 1923 Hague Rules of Aerial Warfare

Naval Warfare
* 1907 Hague Convention on the Rights and Duties of Neutral Powers in Naval War
* 1909 Declaration Concerning the Laws of Naval War

War Spy
* 1899 Hague Convention
* 1949 Geneva Convention IV Relative to the Protection of Civilian Persons in Time of War
* 1977 Geneva Protocol I

Cyberespionage
None